Three Fundamental Questions on Data Classification Compliance

By David Pan | Nigel Zhu | Susan Deng | Stella Huang

Recently, China has intensively promulgated regulations and draft guidance documents on data classification and grading system (see Chart 1). These regulations and documents purport to refine the data classification and grading system stipulated in the regulations already in effect, and provide specific guidance to government departments and organizations to implement the classification and grading system. From the angle of corporate compliance, it is also necessary for enterprise to fulfill complex data compliance obligations based on data classification and grading system. In this article, by "separating the wheat from the chaff" from a very complex legal regime, we briefly analyze three fundamental questions.

(1) What is data classification and grading system?
(2) Why to implement the system?
(3) How to implement the system?

1. What is data classification and grading system

In addition to the important data classification system stipulated in the *Data Security Law*, various departments and regional governments are gradually formulating data classification rules or guidelines for different sectors to provide reference for enterprises to implement data classification and grading system.

According to Article 21 of the *Data Security Law* effective on September 1, 2021, the State establishes a data classification and grading protection system to protect data by category and by grade, depending on the importance of the data in economic and social development, and the damage caused to national security, public interests, or the legitimate rights and interests of individuals and organizations if the data is falsified, damaged, disclosed, illegally obtained or illegally used. The national data security coordination mechanism shall coordinate the relevant departments to formulate catalogs of important data, and strengthen the protection of important data. Data concerning national security, lifelines of the national economy, important people's livelihood, major public interests, etc. are core data of the State, and shall be subject to a stricter management system. All regions and departments shall, under the data classification and grading protection system, determine the specific catalogue of important data for their respective regions and departments and for relevant industries and fields, and give priority to the protection of data included in the catalogue.

Data classification and grading system does not apply to important data only. The system guides enterprises to (i) classify all the data which they possess according to laws and regulations and the actual situations of the enterprises themselves, and (ii) on the basis of such classification, manage such data according to the importance and severity of "disaster consequences" of different categories of data.

Followed by the important data classification system, data classification and grading system is evolving, which includes mainly the following regulations, normative documents and policies.

Issuing authority	Laws and regulations
Standing Committee of the National People's Congress	Data Security Law
Ministry of Industry and Information Technology	Measures for the Management of Data Security in the Field of Industry and Informatization (Trial) (Exposure Draft)
Ministry of Industry and Information Technology	Notice on Strengthening Cyber Security and Data Security in the Internet of Vehicles
Standing Committee of Shanghai Municipal People's Congress	Data Regulations of Shanghai (Draft) (Exposure Draft)
National Information Security Standardization Technical Committee	Cyber Security Standard Practice Guide - Data Classification and Grading Guidelines (Exposure Draft)
Standing Committee of Guizhou Provincial People's Congress	Big Data Security Regulations of Guizhou Province
Tianjin Cyberspace Administration of China	Measures for the Management of Data Security of Tianjin (Trial)
General Office of the State Council	Measures for the Management of Scientific Data
China Securities Regulatory Commission	Measures for the Information Technology Management of Securities and Fund Operators Data Classification Guidelines for Securities and Futures Industry (JRT 0158-2018)

Ministry of Industry and Information Technology	Guidelines for Classification and Grading of Industrial Data
People's Bank of China	Personal Financial Information Protection Technical Specification (JR/T0171-2020)
People's Bank of China	Financial Data Security – Guidelines for Data Security Classification (JR/T 0197-2020)

Chart 1, Major regulations and documents on data classification and grading system

2. Why to implement the system

From the perspective of regulatory supervision, it is imperative to implement data classification and grading system so as to enforce the regulatory requirements on important data and others supervised data set forth in the *Cyber Security Law*, the *Data Security Law*, the *Personal Information Protection Law* and other laws and regulations. At the same time, data classification and grading can also facilitate the regulator's policy to promote the opening and sharing of data and enhance the value of data resources.

From the perspective of corporate compliance, enterprises not only face compliance obligations relating to personal information and important data, but also special categories of data applicable in their industries and fields. If an enterprise does not conduct a thorough assessment on its possessed data and manage data by category and by grade accordingly, it would be extremely difficult (if not impossible) to fulfill data compliance obligations.

As a data processor, an enterprise must fulfill its legal obligation of data classification and grading. In addition, in order to fulfill various data compliance obligations regarding personal information protection, data collection and use, data export, and important data, it is necessary for the enterprise to properly implement data classification and grading. In accordance with relevant laws and regulations, an enterprise that fails to perform data classification and grading obligations may be subject to administrative penalties such as discredit record, public exposure, confiscation of illegal income, fines, suspension of business, suspension for rectification, closure of websites, revocation of licenses and permits, or revocation of business licenses; and if a crime is constituted, criminal liability shall be investigated in accordance with the law.

For enterprises in specific industries (for example healthcare industry undertakings), certain internal business data (for example, population health information and human genetic resource information) may constitute specially regulated data. Failure to separately process and protect such data may cause a violation of special laws and regulations.

Currently, the relevant regulations and documents are still in the draft exposure stage. Enterprises naturally wonder whether they should wait until the relevant regulations and documents become effective to implement data classification and grading. Judging from legislation and law enforcement practices, we recommend that enterprises should NOT take a "wait and see" attitude. Rather, it is advisable for enterprises

to proactively implement data classification and grading. First, as a new legal branch, China's legislation on data classification and grading system has been "crossing the river by feeling the stones", and its legislative logic has also undergone a change from "bottom-up" to "top-down" (see our previous article *The Stronger Ability, the Greater Responsibility - A Review of the Data Classification and Grading System*). The newly released *Cyber Security Standard Practice Guide - Data Classification and Grading Guidelines (Exposure Draft)* includes several specific principles of data classification and grading, one of which is the principle of "autonomy". That is, under the State's framework of data classification and grading rules, and according to specific management needs, industries, fields, localities or organizations shall independently refine and determine the categories and grades of data under their own jurisdictions. Therefore, under the premise that the framework rules are basically completed, enterprises should start considering refinement on their own; secondly, as mentioned above, enterprises must thoroughly sort out the data which they possess, implement data classification and grading system, and take different control and protection measures for data of different importance and sensitivity levels, establish and improve the internal process of data risk management. Doing so will help enterprises fulfill other obligations regarding cyber security and data compliance.

3. How to implement the system

By referring to relevant laws and regulations and law enforcement practices, we summarize the hardcore for enterprises to implement data classification and grading.

(1) Establish a joint taskforce composed of personnel from departments of legal and compliance, IT, and business

To implement data classification and grading, it is necessary to complete tasks such as identifying data, understanding regulatory requirements, identifying objects harmed by data incidents and degree of harm, which require the joint efforts of legal and compliance, IT, and business personnel.

For example, an enterprise often possesses structured data (RDD, SQL, NOSQL, JSON, etc.), semi-structured data (log files, XML documents, Email, etc.), and unstructured data (office documents, text, pictures, HTML, reports, images, audio and video materials, etc.). Structured and semi-structured data may be "unreadable" for legal and compliance personnel and business personnel. Interpretation of these data requires the support from the enterprise's IT department; on the other way around, IT department relies on the professional interpretation of the legal and compliance department on legal and compliance requirements. Even seemingly basic legal issues require a professional advice. For example, the identification of the scope of personal information (which is protected by law) must be performed based on laws, regulations, judicial practices and enforcement practices; analysis of the consequences of data tampering, destruction, and leakage depends on the business department's detailed explanation on the data source, purpose, impact on upstream and downstream industries, etc.

(2) Classify data

According to relevant laws and regulations, enterprises should first classify and then grade data, classify and label data according to factors such as industry requirements, business needs, data sources and uses, formulate data classification lists and regularly update the lists.

Generally, an enterprise can classify its possessed data into three categories: public data, personal information, and enterprise data. Each category of data can be further subdivided according to laws and regulations, and enterprises' own needs and actual conditions.

Categories of data	Definition of the categories of data	Examples
Public data	Data collected and generated by public management and service agencies in the process of performing public management and service duties in accordance with the law, and data collected and generated by other organizations and individuals in the process of providing public services which relates to public interests	Government affairs data, data in the process of providing public services such as water supply, power supply, gas supply, heat supply, public transportation, elderly care, education, medical and health, postal services, etc. which relates to public interests
Personal information	All kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously	Personal identification information, personal biometric information, personal property information, personal communication information, personal location information, personal health and physiological information
Enterprise data	Data collected and generated by enterprises in R&D and design, manufacturing, operation management, operation and maintenance services, platform operations, application services, and internal management	Business data, business management data, system operation and security data

Chart 2, Categories of data

(3) Grade data

Enterprises can refer to the data grading rules set forth in the *Cyber Security Standard Practice Guide - Data Classification and Grading Guidelines (Exposure Draft)*, classify various categories of data as ordinary data (Levels 1 to 3), important data (Level 4) and core data (Level 5). If certain data spans more than one level, then it should be graded at a highest level.

Objects harmed by data incidents / Degree of harm	National security	Public interests	Organizations' legitimate interests	Individuals' legitimate interests
Major serious harm	Core data (Level 5)	Core data (Level 5)	Important data (Level 4)	Important data (Level 4)
Serious harm	Core data (Level 5)	Important data (Level 4)	Ordinary data (Level 3)	Ordinary data (Level 3)
Ordinary harm	Important data (Level 4)	Ordinary data (Level 3)	Ordinary data (Level 2)	Ordinary data (Level 2)
Minor harm	Important data (Level 4)	Ordinary data (Level 2)	Ordinary data (Level 1)	Ordinary data (Level 1)

Chart 3, Data grading rules

Undoubtedly, it is important for enterprises to determine whether the data they possess belongs to core data and important data. If an enterprise possesses core data and important data, it must manage such data in accordance with laws and regulations. Taking pharmaceutical enterprises as an example, enterprises can consider the following two steps for conducting the assessment.

Step one: Whether enterprises possess any of the following data:

- Related to infectious diseases, new biotechnology, laboratory biology, important national genetic resources and genetic data;
- Related to emergent infectious diseases, major animal and plant epidemics, microbial resistance, and biotechnology environmental safety;
- Personal privacy, patient and reporter information obtained during the reporting and monitoring of adverse drug and contraceptive reactions;
- Personal privacy and related disease and epidemiological information of infectious disease patients and their families and close contacts obtained during the monitoring of public health emergencies and infectious disease epidemics;
- Various types of diagnosis, treatment, and health data information such as personal electronic medical records and health files kept by medical institutions and health management service institutions;
- Personal information of human organ donors, recipients and applicants for human organ transplantation in the medical service of human organ transplantation;
- Personal information of sperm and egg donors and users in human assisted reproductive technology services and applicants for such services;
- Personal privacy involved in the process of family planning services;

- Genetic information of individuals and families;
- Life registration information.

Step two: Analyze the degree of harm to national public health security and interests, the business service capabilities of enterprises and upstream and downstream industries, and individuals' legitimate rights if such data is tampered, destroyed, leaked, or illegally obtained or used illegally, and identify the grade of data, by referring to Chart 3.

(4) Manage data by category and by grade

After data classification and grading are completed, enterprises shall perform external and internal compliance obligations in accordance with laws and regulations. Externally, enterprises shall perform filing and data security assessment obligations etc. to the regulatory authorities. Internally, enterprises shall manage data by category in accordance with the data CIA principles (i.e., confidentiality, integrity, and accessibility).

If you would like to know more information about the subjects covered in this publication, please contact:

David Pan
+86 21 3135 8701
david.pan@llinkslaw.com

SHANGHAI
19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

SHENZHEN
18F, China Resources Tower
2666 Keyuan South Road, Nanshan District
Shenzhen 518063 P.R.China
T: +86 755 3391 7666
F: +86 755 3391 7668

HONG KONG
Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON
1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD